

# MICHIGAN STATE UNIVERSITY

July 8, 2016

Federal Communications Commission  
445 12th Street SW, Washington, DC 20554

RE: Study Submitted To: "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," WC Docket No. 16-106

To Whom It May Concern:

Enclosed please find a copy of a new study I recently co-authored with Dr. Anne Oeldorf-Hirsch entitled "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services." The study, currently under peer review, demonstrates the extent to which individuals ignore privacy policies and terms of service policies when engaging with social networking services. While numerous studies have previously addressed the extent to which users understand policies and how long it might take to read policies, little evidence previously existed demonstrating empirically that users often ignore these policies. The results suggest that the 'notice and choice' privacy model does not adequately provide the necessary deliverables to ensure protections. Transparency and access are terrific places to start, but terrible places to finish. More needs to be done to ensure that users are aware of what they are agreeing to, and protected from threats associated with data sharing and data use, especially when it comes to eligibility decision-making.



**College of  
Communication  
Arts & Sciences**

**Department of  
Telecommunication,  
Information Studies,  
& Media**

404 Wilson Road  
Room 409  
East Lansing, MI  
48824

517-355-8372  
Fax: 517-355-1292  
[tisminfo@msu.edu](mailto:tisminfo@msu.edu)  
<http://tism.msu.edu>

Here is a copy of the study abstract:

This paper addresses 'the biggest lie on the internet' with an empirical investigation of privacy policy (PP) and terms of service (TOS) policy reading behavior. An experimental survey ( $N=543$ ) assessed the extent to which individuals ignore PP and TOS when joining a fictitious social networking site, NameDrop. Results reveal 74% skipped PP, selecting 'quick join.' For readers, average PP reading time was 73 seconds, and average TOS reading time was 51 seconds. A regression analysis revealed information overload as a significant negative predictor of reading TOS upon signup, when TOS changes, and when PP changes. Qualitative findings further suggest that participants view policies as nuisance, ignoring them to pursue the ends of digital production, without being inhibited by the means. Implications were revealed as 98% missed NameDrop TOS 'gotcha clauses' about data sharing with the NSA and employers, and about providing a first-born child as payment for SNS access.

Please feel free to contact me, should you require any further information.

Sincerely,

A handwritten signature in black ink, appearing to read "Jonathan A. Obar".

Jonathan A. Obar, PhD  
Research Associate, Quello Center for Telecommunication Management and Law  
Michigan State University  
[obar@msu.edu](mailto:obar@msu.edu)

Running Head: BIGGEST LIE ON THE INTERNET

**The biggest lie on the internet: Ignoring the privacy policies and terms of service  
policies of social networking services**

Jonathan A. Obar\*

Anne Oeldorf-Hirsch\*\*

\*York University; Quello Center, Michigan State University

\*\*University of Connecticut

WORKING PAPER

July 7, 2016

**The biggest lie on the internet: Ignoring the privacy policies and terms of service  
policies of social networking services**

**ABSTRACT**

This paper addresses ‘the biggest lie on the internet’ with an empirical investigation of privacy policy (PP) and terms of service (TOS) policy reading behavior. An experimental survey ( $N=543$ ) assessed the extent to which individuals ignore PP and TOS when joining a fictitious social networking site, NameDrop. Results reveal 74% skipped PP, selecting ‘quick join.’ For readers, average PP reading time was 73 seconds, and average TOS reading time was 51 seconds. A regression analysis revealed information overload as a significant negative predictor of reading TOS upon signup, when TOS changes, and when PP changes. Qualitative findings further suggest that participants view policies as nuisance, ignoring them to pursue the ends of digital production, without being inhibited by the means. Implications were revealed as 98% missed NameDrop TOS ‘gotcha clauses’ about data sharing with the NSA and employers, and about providing a first-born child as payment for SNS access.

**The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services**

Effective strategies for realizing digital reputation and privacy protections remain unclear. While self-governance efforts by proprietary platforms provide de facto protections (DeNardis and Hackl, 2015), leaving privacy and reputation to companies monetized through data-driven business models seems problematic. Data resistance technologies and other privacy-enhancing services offer the possibility of bottom-up protections; however, ubiquitous and continuously effective adoption in the face of the Big Data deluge seems an unattainable ideal (Obar, 2015). Others simply suggest that privacy is dead (Sanders, 2011; Morgan, 2014). Differing from these strategies defined by neoliberalism and futility is another approach to solving difficult problems - government intervention.

Top-down approaches to privacy and increasingly reputation protections by governments throughout the world often draw from a contentious model referred to as the 'notice and choice' privacy framework. Notice and choice evolved from the U.S. Federal Trade Commission's (FTC) Fair Information Practice Principles, developed in the 1970s to address growing information privacy concerns raised by digitization. In the early 1980s, the FIPPs were promoted by the OECD as part of an international set of privacy guidelines (OECD, 1980), contributing to the implementation of data protection laws and guidelines in the U.S., Canada, the EU, Australia and elsewhere, often with language mirroring the FIPPs from the 1970s. Even in the face of considerable criticism (see: Cate, 2006; Solove, 2012; Reidenberg et al, 2015; Obar, 2015), ongoing efforts to strengthen data protections continue to draw on the old framework.

## BIGGEST LIE ON THE INTERNET

The notice and choice privacy framework was designed to “put individuals in charge of the collection and use of their personal information” (Reidenberg et al, 2014: 3). Though implementation differs by context, the choice components consist of a variety of access, control and security mechanisms that recommend how users might check, correct and/or approve personal data managed and used by different organizations, similar to how one monitors credit reports before applying for a loan.

The focus of our current inquiry however is on the notice component, noted by the FTC as “the most fundamental principle” (FTC, 1998: 7) of personal information protection. Notice consists of efforts by an entity to inform the source of data collection, sharing, etc. that the action in question is taking place. As the FTC (1998) notes, choice and related principles attempting to offer data control “are only meaningful when a consumer has notice of an entity’s policies, and his or her rights with respect thereto.” (7) Notice policies typically include language drawn from the OECD’s “openness principle” which states:

[t]here should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. (OECD, 1980)

Across contexts, entities involved in data management attempt to abide by notice policy by providing individuals with consent materials, typically in the form of privacy policies and terms of service policies. These policies appear on websites, applications, are sent in the mail, provided in-person, generally when an individual connects with the entity in question for the first time, and increasingly when policies change. Despite suggestions

## BIGGEST LIE ON THE INTERNET

that notice policy in particular is deeply flawed (e.g. McDonald and Cranor, 2008; Reidenberg et al, 2015; Obar, 2015), strategies for strengthening notice policy continue to be seen as central to addressing, for example, privacy concerns associated with corporate and government surveillance, and consumer protection concerns about Big Data, data brokerage and eligibility decision-making (see: FTC, 2012).

This brings us to the biggest lie on the internet, which anecdotally, is known as “I agree to these terms and conditions.” The term “anecdotally” is chosen deliberately in this context, as much of the evidence of the biggest lie, to this point, comes in the form of anecdote. Upon discussing the current study with colleagues, most agree that ignoring privacy and terms of service (TOS) policies is both a reality and a problem. “I never read those things” and “nobody reads them” are common responses. The non-profit ToS;DR (Terms of Service; Didn’t Read) advances a similar anecdotal assertion. The front page of their website reads “‘I have read and agree to the Terms’ is the biggest lie on the web. We aim to fix that.” A less well-known site, [www.biggestlie.com](http://www.biggestlie.com) states on its site “Let’s STOP the biggest lie on the web!” and asks users to confess and protest against the lie by clicking “I confess – and protest!” – about 4,500 such confessions have been made since 2012. In both cases, neither organization cites any academic research to substantiate their claims.

Policymakers often advance a similar unsubstantiated claim. For example, in 2007 FTC Commissioner Jon Leibowitz said, without citing any empirical evidence,

Initially, privacy policies seemed like a good idea. But in practice, they often leave a lot to be desired. In many cases, consumers don’t notice, read, or understand the privacy policies. (Leibowitz, 2007: 4)

## BIGGEST LIE ON THE INTERNET

A 2010 report on data privacy by the Department of Commerce noted, again without citing empirical evidence, “The shortcomings of many privacy policies [...] are widely recognized: they can be [...] “overwhelming” to the few consumers who actually venture to read them.” (DOC, 2010: 32) A recent FTC privacy report similarly noted, “Recent research and surveys suggests that many consumers [...] do not read or understand privacy policies” (FTC, 2012: 61). One survey, conducted by Zogby International (no evidence of peer review provided) was referenced, summarized in a comment submitted to the FTC by Common Sense Media. The comment however makes no mention of users ignoring policies, but instead notes that individuals would “take more time to read” policies if they were shorter and clearer (CSM, 2010: 1).

Whether or not the magnitude of the lie is to the degree the anecdote suggests, the idea that the practice of ignoring privacy and TOS agreements is common knowledge, points to considerable regulatory failure. If it is true that people typically ignore policies when engaging digital media, it suggests that notice policy doesn’t work, and perhaps that committed and continued resources devoted to notice efforts are being wasted.

Acknowledgment of this regulatory failure would be a first step towards more pragmatic approaches that might actually provide protections. Before such an acknowledgement can be made however, the extent to which individuals ignore privacy and terms of service policies when engaging with digital media services ought to be addressed.

This survey analysis of 543 participants addresses the extent to which individuals ignore privacy and terms of service policies when joining social media services for the first time as well as when policies are updated. It also addresses the reasons individuals ignore

policies. In what follows, a review of the brief available literature on privacy and TOS policy engagement will be discussed. This is followed by the survey analysis.

### **The Debate Over Notice Policy**

The desire to understand and promote connections between the informed individual and self-governance precedes discussions of digital data. For example, in 1822, James Madison, considered the 'Father' of the U.S. Constitution and Bill of Rights wrote:

A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives. (Madison, 1822)

With these words, Madison buttressed subsequent regulatory efforts aimed at promoting corporate and government transparency, and helped carve a path to the U.S. Freedom of Information Act and beyond (Schudson, 2015). Indeed, access to information, and openness about procedures and processes that impact an individual have historically been viewed as essential to ensuring autonomy and liberty, not only in the political context, but in the consumer context as well (Bowles, Hamilton and Levy, 2013). The normative regulatory philosophy embedded within efforts to promote transparency assumes that the voice of the average individual can provide a check on institutional power structures, protect against economic, social and even moral stratifications, bias and in some instances, tyranny (Walker, 1966; Gramberger, 2001; Obar 2010). As a result, "transparency is thus a highly valued instrumental good, since it is an input into a process of monitoring that increases the odds that voters or consumers get what they want from institutional actors." (Bowles et al, 2013: xv). These views continue to be espoused today, with fears associated



with removal of notice components linked to the loss of benefits historically linked to transparency, namely, liberty, autonomy and the ability to hold those in power to account (see: OPC, 2016). This assumes, perhaps incorrectly, that by maintaining notice policy that additional protections result – this remains unclear.

While some of the strongest research looking at user engagement with privacy policies addresses the extent to which users understand them (Reidenberg et al, 2015) and how long it takes to read them (McDonald and Cranor, 2008), empirical evidence demonstrating the extent to which users ignore privacy and terms of service policies is lacking, especially in the context of social networking services.

An often-cited book chapter by Cate (2006) entitled *The Failure of Fair Information Practice Principles* does provide some empirical support to the idea that individuals ignore policies; however, the evidence provided is now dated and generally tangential to current concerns. Cate notes that “an avalanche of notices and consent opportunities [...] are widely ignored by the public” (360). To substantiate this assertion Cate begins by citing a 1997 study from the U.S. Postal Service which suggests that 52 percent of unsolicited mail in the U.S. is never read. This is followed by what appears to be anecdotal evidence from 2002 in which an unnamed ISP noted that 58 percent of its marketing emails remain unopened. The conflation of opening snail mail and marketing emails with privacy and TOS policy engagement is problematic; however, the suggestion that there are challenges getting people to read things they may not want to does somewhat advance the argument. Cate goes on to discuss how in 2001 the chief privacy officer of ISP Excite@Home noted during an FTC workshop “that the day after *60 Minutes* featured his company in a segment on Internet privacy, only 100 out of 20 million unique visitors to its website accessed that

company's privacy pages" (c.f. Cate, 2006: 261). Data from Yahoo is then presented noting that an average of 0.3 percent of users accessed its privacy policy in 2002, with the number rising to 1 percent during a privacy-publicity "firestorm." Cate provides one additional piece of statistical evidence to support the assertion, describing how in 2001, in response to the Gramm-Leach-Bliley of 1999, at least 2 billion privacy notices were mailed from tens of thousands of financial institutions to consumers. According to Cate, these efforts were supported by considerable press coverage and promotion by privacy advocates. Apparently in mid-2001, less than 5 percent of consumers had opted out of data sharing agreements, and a September survey noted that 35 percent of respondents "could not recall even receiving a privacy notice" (Ibid: 361-362). In sum, while Cate's empirical evidence begins to support the argument, it is clear that more data is needed, especially since the majority of the evidence provided predates social media and the Big Data boom.

Milne and Culnan (2004) present perhaps the best empirical assessment of readers versus non-readers of privacy policies to date, noting "the literature has not examined the tendency to read notices" (17). Their results suggest that 17.3 percent of the 2,468 individuals surveyed were identified as "non-readers," while 83.7 percent of those surveyed read the policies. Of the readers, 33.3 percent noted that they "rarely read online privacy notices." It should be added that the authors ran their survey in 2001, which suggests again that data representing the current landscape is lacking.

One other example worth noting is found in Nissenbaum's (2009) seminal work *Privacy in Context*. She devotes a section in her book to an issue known as the privacy paradox (Norberg, Horne and Horne, 2007) "a stark contradiction at whose heart is this: people appear to want and value privacy, yet simultaneously appear not to value or want

it.” (Nissenbaum, 2009: 104) In describing one component of this paradox, specifically that “only 20 percent of users claim to read privacy policies ‘most of the time’” (105), Nissenbaum cites a press release of a study by TRUSTe from 2006, a self-described leading Data Privacy Management company (TRUSTe, 2006).

The lack of peer-reviewed academic research in this area suggests a considerable research gap, and the need for empirical evidence. In this paper we conduct an empirical assessment of the extent to which individuals ignore privacy and TOS policies when engaging SNS. We address the following research questions:

RQ1: To what extent will participants ignore privacy and terms of service policies for the fictitious social networking service NameDrop?

RQ2: To what extent will participants fail to notice ‘gotcha’ clauses in the NameDrop policies?

RQ3: To what extent will participants read privacy and terms of service policies for real social networking services?

RQ4: What attitudes about privacy and terms of services policies predict the extent to which participants ignore them?

## **Method**

### **Sample**

Participants ( $N = 543$ ) consisted of undergraduate students recruited from a large communication class at a university in the eastern United States. The sample was 47% female, 45% male (8% unclear), and the average age was 19 years. Sixty-two percent of participants identified as Caucasian, 15% Asian, 6% Black, 2% Hispanic or Latino/a, 3% as mixed race/ethnicity, and 3% as another race/ethnicity (9% unclear). All participants

received course credit for completing the survey, hosted on [www.qualtrics.com](http://www.qualtrics.com) in fall 2015.

## **Procedure**

The survey consisted of two sections: (1) quantitative and qualitative assessments of participant interaction with a privacy and a TOS policy for a fictitious SNS, and (2) a self-report section about reading privacy and TOS policies for real SNS. To complete (1) researchers developed the front page for a fictitious SNS called “NameDrop” (see Figure 1), a hypothetical competitor of LinkedIn.

[Figure 1 About Here]

### **Section 1: Participant interaction with NameDrop Privacy and TOS Policies**

Participants were informed that their university was working with NameDrop and that they would be contributing to a pre-launch evaluation of the SNS. This deception aimed to convince participants that the evaluation would involve: signing-up, reviewing the SNS, and deleting their account if desired. At no point was it stated that personal information would be removed upon deletion. At no point was an SNS evaluated. After consenting, the ‘sign-up’ process involved only an encounter with the NameDrop policies.

After viewing NameDrop’s front page (see Figure 1), participants were given what we term a ‘quick-join’ option, allowing them to skip the privacy policy without reading it. Quick-join options are common to SNS, including Facebook, Google, Twitter and LinkedIn. Participants could choose “Sign Up! (By clicking Sign Up, you agree to NameDrop’s privacy policy)” or “Click here to read NameDrop’s privacy policy.” After skipping or reviewing the policy, participants were asked to review NameDrop’s TOS. Both policies could be accepted or rejected.

## BIGGEST LIE ON THE INTERNET

The NameDrop policies were modified versions of LinkedIn's to ensure comparable length to current SNS. In addition to assessing accept/reject, the software timed how long participants spent on each policy. The privacy policy measured 7,977 words and the TOS 4,316 words. The literature suggests that average adult reading speed, for individuals with a grade 12 or college education is approximately 250-280 words per minute (Taylor, 1965). This suggests that it should take the average adult between 29 and 32 minutes to read NameDrop's privacy policy and 15 and 17 minutes for TOS.

Two 'gotcha' clauses were added to TOS to further assess ignoring behavior. The intention was to present clauses so outrageous that concern would be expressed after reading. The first clause dealt with data sharing, the NSA and eligibility determinations:

3.1.1 NameDrop Data [...] Any and all data generated and/or collected by NameDrop, by any means, may be shared with third parties. For example, NameDrop may be required to share data with government agencies, including the U.S. National Security Agency, and other security agencies in the United States and abroad. NameDrop may also choose to share data with third parties involved in the development of data products designed to assess eligibility. This could impact eligibility in the following areas: employment, financial service (bank loans, insurance, etc.), university entrance, international travel, the criminal justice system, etc. Under no circumstances will NameDrop be liable for any eventual decision made as a result of NameDrop data sharing.

The second clause was more extreme, stating that by agreeing to TOS, participants would give up their first-born child to NameDrop:

2.3.1 Payment types (child assignment clause): In addition to any monetary payment that the user may make to NameDrop, by agreeing to these Terms of Service, and in exchange for service, all users of this site agree to immediately assign their first-born child to NameDrop, Inc. If the user does not yet have children, this agreement will be enforceable until the year 2050. All individuals assigned to NameDrop automatically become the property of NameDrop, Inc. No exceptions.

Open-ended questions were posed asking whether participants had any concerns about the policies and also about perceptions of quick-join options.

A coding instrument was utilized to assess the answers to the open-ended questions. Variables 1-5 identified concerns associated with the NameDrop privacy and TOS policies (including data sharing, the NSA, the child assignment clause, the policy length and general concern). Variables 6-7 identified whether quick-join options are utilized often or sometimes. Inter-coder reliability was conducted using two trained coders reviewing responses from 119 participants (22% of total). Holsti's (1969) percentage agreement test revealed inter-coder reliability scores ranging from  $p = .97$  to  $p = 1.00$ , with an average across the seven variables of  $p = .99$ .

## **Section 2: Self-Report Reading of Real SNS Privacy and TOS Policies**

*Time spent reading privacy policies.* Participants were asked how many minutes (on a slider ranging 0-60 minutes) they spent reading privacy and TOS policies for the following services upon signup and again when policies change: Facebook, Twitter, Instagram, Skype, SnapChat, Yik Yak, Xbox Live, iPhone Messenger, Gmail and iTunes. All provide SNS functionality, except iTunes, which was selected to assess behaviors associated with a different digital service.

*Privacy and TOS policy reading behaviour.* Four matched pairs of items (8 items total) measured participants' privacy policy and TOS reading behavior: "I agree to privacy policies/Terms of Service agreements without reading them," "I skim privacy policies/Terms of Service agreements," "I read privacy policies/Terms of Service agreements thoroughly" and "I review privacy policies/Terms of Service agreements when notified that there have been updates". These were measured as 7-point Likert-type scale items (Strongly Disagree – Strongly Agree). For both scales, reliability was improved when the "I skim" item was removed, resulting in reliable three-item scales for privacy policy ignoring,  $\alpha = .78$ , and TOS ignoring,  $\alpha = .75$ .

*Privacy and TOS policy attitudes.* Sixteen matched pairs of items (32 items total) were developed to measure participants' attitudes toward the policies. These items were factor analyzed using Principal Axis Factoring and Varimax rotation, revealing a three-factor structure. Using a criterion of items loading at .5 or higher on one factor with no cross-loadings of .5 or higher on other factors, 23 items loaded onto the three factors, explaining 42% of the variance. See full scales and factor items in Table 1.

*Demographics.* Participants were asked to indicate their age, gender, and race/ethnicity.

## Results

### Section 1: Participant Interaction with NameDrop Privacy and TOS Policies

RQ1 was addressed by recording whether participants skipped the NameDrop privacy policy via a 'quick-join' option, and then the extent to which they read the privacy policy (for those declining 'quick-join') and TOS policy.

#### *The 'Quick-Join' Option*

## BIGGEST LIE ON THE INTERNET

Upon encountering the quick-join option for the NameDrop privacy policy, 399 of 543 participants (74%) accepted the option and skipped reading the privacy policy entirely. This means that these participants accepted NameDrop's privacy policy without seeing or reading any part of it.

To expand upon this finding, responses to open-ended questions about quick-join options were assessed. From the 527 participants that provided qualitative responses, 411 (78%) said they use the quick-join method often. Of the remaining participants, 17 suggested that they sometimes quick-join. Removing responses labeled "unclear" (most of these were critical of the process of reading policies but didn't answer the question), more than 90 percent of those surveyed said they use quick-join options often or sometimes, with the vast majority using them often.

Participants noting that they often use quick-join options usually provided an explanation. An overarching theme present in many of the responses suggests that participants are generally uninterested in the notice component of SNS. The quick-join option was often praised for making the notice process "easy," "quick," "simple," and "convenient." One participant noted, "it expedites the process." Participants were critical of the policies themselves, suggesting that they are "too long" and "wordy." Feelings of apathy as well as futility were common, with the latter sometimes linked to the perception that policies wouldn't be understood even if they were read.

Expanding upon the "quick" and "easy" comments was the suggestion that participants are disinterested in the notice process because it is perceived as an unwanted and/or unnecessary barrier between the user and the desired SNS experience. One participant justified using the quick-join option by saying, "regardless of the policy, if a



mass majority of my friends and family are on the networking site I want to be included as well in order to interact with them.” Another noted, “my friends use this social media in order (sic) to catch up with their life i (sic) signup for this as quick as possible.” Indeed, the desire to enjoy the ends of digital media production without being inhibited by the means was clear, with one participant noting “I’m in a hurry to use the service,” while another said “its a hassle to deal with a massive amount of boring pages about privacy and security when the site you are joining is there to do something much more interesting.” Indeed, the perception that these attitudes are the norm was acknowledged, “it feels like a cultural norm not to read them and I’m too lazy to read them in detail.”

### **Reading or Ignoring NameDrop Policies**

The average adult reading speed for individuals with a grade twelve or college education is approximately 250-280 words per minute (Taylor, 1965). This suggests that it should take between 29 and 32 minutes to read the NameDrop privacy policy (7,977 words). The actual time spent reading ranged from 2.96 seconds to 2220.67 seconds (37 minutes), with a median of 13.60 seconds ( $M = 73.72$ ,  $SD = 237.26$ ). As noted in Figure 2, 80% of participants spent less than one minute reading the NameDrop privacy policy, with an additional 14% percent reading for less than five minutes.

The NameDrop TOS was 4,316 words, suggesting it should take 15 to 17 minutes. Participants read between 3.48 seconds to 6699.35 seconds at most (111 minutes) with a median of 14.04 seconds ( $M = 51.12$  seconds,  $SD = 297.93$ ). Similar to the privacy policy, 86% of participants spent less than one minute reading the TOS, with an additional 11% spending less than five minutes (Figure 2). In sum, 96% of participants spent less than 5 minutes on the NameDrop privacy policy and 97% spent less than 5 minutes on TOS.

[Figure 2 About Here]

### **The “Gotcha” Clauses in the NameDrop Terms of Service Policy**

RQ2 was assessed by coding open-ended responses about NameDrop’s privacy and TOS policies for any mention of the “gotcha” clauses. These responses revealed that just 83 participants (15%) had concerns about the policies. Of those, nine (1.7% of those surveyed) mentioned the child assignment clause and 11 (2%) mentioned concerns with data sharing; however, only one of the 11 mentioned the NSA. The remainder of the comments dealt with a variety of concerns including the length of the policies, and the trustworthiness of the SNS.

Despite these concerns, and the finding that policy-reading times were well below the expected average, 100% of participants agreed to both policies.

### **Section 2: Self-Report Reading of Real SNS Privacy and TOS Policies**

RQ3 was addressed by averaging reported time spent reading the TOS and privacy policies for various services when participants sign up and when policies change. Thirty-nine percent of participants stated they never read TOS agreements for any services when signing up. For each given service, 52-65 percent stated that they ignore the TOS completely (spend zero minutes reading it) when signing up. For those that do read policies, reported time spent ranged from 1 minute to 43 minutes ( $M = 4.68$ , Median = 2.00).

Reading times for privacy policies showed a similar pattern. Thirty-five percent of participants acknowledged not reading the privacy policy for any services when signing up. For any given service, 42-67 percent ignored the privacy policy when signing up. Reported

time spent reading ranged from 1 minute to 60 minutes ( $M = 4.91$ , Median = 2.35). Reading patterns when TOS and privacy policies change were similar.

### **What Predicts Time Spent Reading Policies**

The factor analysis revealed three attitude factors. The first, *Information overload* (10 items,  $\alpha = .90$ ), contained items about participants perceiving TOS and privacy policies as being too long, too numerous, and taking up too much time. The second factor, *Nothing to hide* (8 items,  $\alpha = .87$ ), drawing on Solove (2007) expressed the idea that the individual in question perceives that policies are irrelevant because the individual is doing nothing wrong, companies will not bother them, and only those who are breaking the rules are affected. The third factor, *Difficult to understand* (5 items,  $\alpha = .85$ ), indicated that individuals perceive that they are unable to understand the language in TOS and privacy policies (see Table 1).

[ Table 1 About Here ]

To answer RQ4, these factors were entered into a hierarchical regression model for the four outcomes: average time spent reading TOS and privacy policies when signing up for a service and when the TOS and privacy policies change. The models included age and gender as control variables in block 1, reported TOS and privacy policy reading behavior in block 2, and the three attitude factors in block 3. See final models in Table 2.

[ Table 2 About Here ]

Of the three factors, Information overload was a significant negative predictor of reading TOS when signing up,  $\beta = -.17$ ,  $p < .01$ , and of reading TOS when they change,  $\beta = -.24$ ,  $p < .001$ . For privacy policies, information overload was a significant negative predictor of reading privacy policies when they change,  $\beta = -.22$ ,  $p < .001$ , but not when signing up for

a new service,  $\beta = -.05$ ,  $p = .38$ . The more individuals experience information overload regarding TOS, and privacy policies when they change, the less time they spent actually reading these policies. However, participants' attitudes that they have nothing to hide and that policies are difficult to understand did not predict reading behavior for TOS or privacy policies. That is, while individuals may hold these beliefs, they have no effect on actual reading behavior.

### Discussion

The results of this study suggest that individuals often ignore privacy and terms of service policies for social networking services. This behavior appears to be common both when signing up to new services and when policies change for services individuals are already using. When people do read policies, they often remain on the relevant pages just long enough to scroll to the "accept" button, and in the few instances where detailed reading takes place, almost all participants demonstrate reading times far below the average reading time needed. It should be kept in mind that the participants described herein are communication students who study privacy, surveillance and Big Data issues in class. If communication scholars-in-training cannot be bothered to read SNS policies, let alone demonstrate concern about the implications of ignoring notice opportunities, it seems likely that the general public would commonly ignore policies as well. Perhaps there is some truth to the "biggest lie on the internet" anecdote.

This study contributes a unique empirical assessment of individuals interacting with the privacy and TOS policies of what they believe to be a real SNS. None of the participants had heard of the service before, and none had any friends or family members to vouch for its quality. All participants were told was that their university had entered into an

agreement with a startup that was interested in having the site tested. The only additional information about the service provided was an image of the service's homepage and that they'd have the option of deleting their profile after completing the evaluation. At no point was it communicated that data collected was to be deleted, an important nuance to the data privacy debate espoused by privacy advocates (Pidd, 2011). Even with no reason to trust the new service, beyond perhaps assumptions about the university's vetting of the startup, or the perception expressed by some participants that all SNS are the same, most of the participants agreed to NameDrop's privacy policy without even looking at it. Of the 543 individuals surveyed, 74 percent accepted the policy via the quick-join option which allowed participants to by-pass the privacy policy without even requiring a glimpse. Qualitative responses suggest that 78 percent of individuals often use the quick-join option and more than 90 percent use it often or sometimes.

Even when participants do not ignore policies, the vast majority barely spends any time reading them. Most appear to take a quick look and then simply scroll to the bottom and click "accept." The NameDrop privacy policy, which is the same length as LinkedIn's policy, should have taken more than half an hour to read; the TOS, more than 15 minutes. Some engaging with NameDrop's privacy and TOS policies spent two and three seconds on the policies, respectively. The average reading time across participants for the privacy policy was 74 seconds, and 51 seconds for the TOS. Though these averages demonstrate reading times well below the time required, the averages were skewed by a few outliers. The median for both privacy and TOS policies is a more accurate representation of the general trend, at approximately 14 seconds for both. Fourteen seconds is hardly enough time to read, understand and provide informed consent to policies between 4,000 and

8,000 words in length. Spending 14 seconds (or 60 seconds for that matter) is akin to not reading the policies at all. Said another way, of those that read the privacy policy, 80% spent less than a minute reading, and 94% less than five minutes. Eighty-six percent of participants spent less than a minute reading the TOS, 97% less than five minutes.

To a lesser degree, but still consistent with the NameDrop analysis, the self-report measures revealed similar findings. When asked about engaging with policies for Facebook, Twitter, Instagram, Skype, SnapChat, Yik Yak, Xbox Live, iPhone Messenger, Gmail and iTunes, 35-39 percent said they ignore policies. Of those that read, the average time reported was about five minutes, with the median approximately two minutes. Though iTunes is not an SNS at the moment, it was revealing to see that the tendency to ignore policies goes beyond SNS engagement and includes other digital media services. This suggests again that, as one participant noted, “it feels like a cultural norm not to read (policies).”

### **The Privacy Paradox**

While almost all participants demonstrated that they either ignore or pay insufficient attention to the policies, the slight differences in reading time between the NameDrop analysis and the self-report analysis do hint at the privacy paradox. The paradox suggests that when asked, individuals appear to value privacy, but when behaviors are examined, individual actions suggest that privacy is not a high priority (Norberg, 2007; Nissenbaum, 2009). To a small degree, this is what was revealed by the analysis. When participants were asked to self-report their engagement with privacy and TOS policies, results suggested average reading times of approximately five minutes. The NameDrop analysis, which tested actual engagement with SNS policies upon signup revealed average

reading times around one minute, with medians of 14 seconds. The qualitative section further suggests what actual privacy behaviors are like, as 98% of participants made no mention of data sharing concerns, and only one participant in the entire study mentioned the NSA. It should be noted that the only NSA mention was in response to the question about concerns associated with the NameDrop policies. This means that it is likely that the one individual who mentioned the NSA was thinking about the NSA because the 'gotcha clause' in the NameDrop policy was noticed. This is an important detail because the likely reason for privacy paradox findings begins with the possibility that individuals express privacy concerns when researchers make participants aware of things like data sharing, the NSA, etc. When researchers are not part of the SNS experience, users are not as likely to be thinking about privacy or data sharing concerns, they are focusing on what they went online to find, SNS affordances.

### **Pursuing the Ends of Digital Production Without Being Inhibited by the Means**

It is important to consider privacy paradox findings in combination with the attitudinal and qualitative analyses. Both analyses suggest a similar finding, that the majority of participants see notice components as nothing more than an unwanted impediment to the real purpose users go online – the desire to enjoy the ends of digital production (i.e. accessing SNS). The only predictor found was a concern over information overload, which included concerns such as “Privacy policies are too long,” “There are too many privacy policies to read,” and “I don't have time to read Terms of Service agreements for every site that I visit.” Privacy and TOS policies were seen as more of a nuisance than anything else.

## BIGGEST LIE ON THE INTERNET

The qualitative assessment reinforced this finding. While a small minority of participants did express privacy concerns, the vast majority praised quick-join options for helping them by-pass notice components. It's not just that privacy and TOS policies are perceived as boring or even pointless, it's that users are going online and engaging with SNS to complete a list of desired tasks, namely, engaging with friends and family online, and all of the other affordances offered by SNS. As one participant noted, "my friends use this social media in order (sic) to catch up with their life i (sic) sign up for this as quick as possible" while another said "it's a hassle to deal with a massive amount of boring pages about privacy and security when the site you are joining is there to do something much more interesting."

It is clear that getting into a legal discussion about data sharing, the NSA and privacy in general is far from the reason that individuals choose to go online. Solove (2012) properly analogizes engagement with policies to the process of students receiving homework. The context Solove refers to is the concern about multiple teachers assigning too much reading, creating a challenging scenario for providing consent. While this analogy correctly describes one of the problems associated with achieving data privacy self-management across all entities involved in data management, the analogy highlights a point more relevant to the current analysis. Users aren't looking for homework when they go online, quite the contrary, it is likely that many users are looking for an escape from their homework when accessing SNS. Users want to engage with the ends of digital production, without being inhibited by an education or a discussion about the means.

The negative implications of this behavior were suggested by the 'gotcha clause' analysis. Instead of notice components helping users control their digital destinies and



corresponding consequences in both online and offline contexts, the vast majority of participants completely missed a variety of potentially dangerous and life-changing clauses. As noted in the first gotcha clause, data could be shared “with government agencies, including the U.S. National Security Agency, and other security agencies in the United States and abroad.” Furthermore, data could be shared “with third parties involved in the development of data products designed to assess eligibility. This could impact eligibility in the following areas: employment, financial service (bank loans, insurance, etc.), university entrance, international travel, the criminal justice system.” These data sharing possibilities are real, and raise a host of expanding concerns associated with data collection and use (see: Pasquale, 2015). Not caring about notice is relevant to Solove’s (2007) critique of the “I’ve got nothing to hide” argument. A common justification for privacy disinterest, this fallacy incorrectly assumes, as one participant in this study noted when justifying quick-join use, “Nothing too bad happened yet, but it's not like I post anything interesting or worthy.” By dismissing responsibility in order to get to the enjoyment of SNS, those who demonstrate Solove’s fallacy ignore possible implications that they might not even be aware of. As Solove notes,

it is hard to claim that programs like the NSA data mining program will not reveal information people might want to hide, as we do not know precisely what is revealed. [...] data mining aims to be predictive of behavior, striving to prognosticate about our future actions. People who match certain profiles are deemed likely to engage in a similar pattern of behavior. It is quite difficult to refute actions that one has not yet done. Having nothing to hide will not always dispel predictions of future activity. (p. 766)

Not only is future behavior difficult to predict, so too are the future uses and concerns associated with the Big Data industry. This is precisely the reason we included the child assignment clause in this study, which more than 98% of participants agreed to without expressing concern. What could be worse than a corporation taking your child away in payment for use of their services? Being ignorant or resigned to the trade-offs associated with digital media usage (see: Turow et al, 2015) is unacceptable if we are to protect ourselves from potential implications now and in the future.

The policy implications of these findings contribute to the community of critique suggesting that notice and choice policy is deeply flawed, if not an absolute failure (Obar, 2015; Reidenberg et al, 2015). Transparency is a great place to start, as is notice and choice policy; however, all are terrible places to finish. They leave digital citizens with nothing more than an empty promise of protection, an impractical opportunity for data privacy self-management, and as Daniel Solove (2012) analogizes, too much homework. This doesn't even begin to address the challenges unique to children in the realm of digital reputation, as if there is little hope for adults, what chance is there for children to protect themselves? More needs to be done to discover pragmatic alternatives that produce privacy and reputation deliverables (see: Obar, 2015). If governments continue to cling to romantic ideals and fallacy, the internet's biggest lie will surely move from anecdote to liability.

### **Works Cited**

Bowles, N, Hamilton, JT and Levy, D (eds) (2013) *Transparency in politics and the media: accountability and open government*. London: IB Tauris.

Cate, FH (2006) The failure of fair information practice principles. In: Winn, JK (ed)

*Consumer Protection in the Age of the Information Economy*. Surrey, UK: Ashgate Publishing, pp. 343-379.

Common Sense Media (2010) Comment submitted to A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era Of Rapid Change, File No. P095416, comment number 00457.

DeNardis, L and Hackl, AM (2015) Internet governance by social media platforms.

*Telecommunications Policy*, 39(9): 761-770.

Department of Commerce (2010) Commercial data privacy and innovation in the internet economy: A dynamic policy framework. Report of The Department of Commerce Internet Policy Task Force.

Federal Trade Commission (1998) Privacy online: A report to Congress. *Washington, DC, June*: 1-71.

Federal Trade Commission (2012) Protecting consumer privacy in an era of rapid change. *FTC report*.

Gramberger, M (2001) Citizens as partners: OECD handbook on information, consultation and public participation in policy making. OECD Report.

Holsti, OR (1969) *Content Analysis for the Social Sciences and Humanities*. Don Mills, Ontario: Addison-Wesley.

Leibowitz, J (2007) *So private, so public: Individuals, the internet & the paradox of behavioral marketing*. Remarks at FTC Town Hall Meeting on “Behavioral Advertising: Tracking, Targeting & Technology” November 1, 2007.

McDonald, AM and Cranor, LF (2008) The cost of reading privacy policies. *ISJLP*, 4: 540-565.

Madison, J (1822) Epilogue: Securing the Republic. James Madison to W.T. Berry, 4 Aug 1822.

Milne, GR and Culnan, MJ (2004) Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3): 15-29.

Morgan, J (2014). Privacy is completely and udderly dead, and we killed it. *Forbes*, 9 Aug.

Nissenbaum, H (2009) *Privacy in context: Technology, policy, and the integrity of social life*. Redwood City, CA: Stanford University Press.

Norberg, PA, Horne, DR and Horne, DA (2007) The privacy paradox: Personal Information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1): 100-126.

Obar, JA (2010) *Democracy or technocracy? An analysis of public and expert participation in FCC policymaking* (Unpublished Doctoral dissertation, The Pennsylvania State University).

Obar, JA (2015) Big Data and The Phantom Public: Walter Lippmann and the fallacy of data privacy self-management. *Big Data & Society*, 2(2): 1-16.

OECD (1980) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

Office of the Privacy Commissioner of Canada (2016) A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act.

- Pasquale, F (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.
- Pidd, H (2011) Facebook could face 100,000 fine for holding data that users have deleted. *The Guardian*, 20 Oct.
- Reidenberg, JR, Russell, NC, Callen, AJ, Qasir, S and Norton, TB (2014) Privacy harms and the effectiveness of the notice and choice framework. *2014 TPRC Conference Paper*.
- Reidenberg, JR, Breaux, T, Cranor, LF, French, B, Grannis, A, Graves, JT, Liu, F, McDonald, A, Norton, TB, Ramanath, R, Russell, NC, Sadeh, N and Schaub, F (2015) Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal*, 30(1): 39-68.
- Sanders, SD (2011) Privacy is dead: The birth of social media background checks. *SUL Rev.*, 39: 243-264.
- Schudson, M (2015) *The Rise of the Right to Know: Politics and the Culture of Transparency, 1945-1975*. Cambridge, MA: Harvard University Press.
- Solove, DJ (2007) 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego law review*, 44: 745-772.
- Solove, DJ (2012) Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126, 1880-1903.
- Taylor, SE (1965) Eye movements in reading: Facts and fallacies. *American Educational Research Journal*, 2(4): 187-202.
- TRUSTe (2006) Consumers have false sense of security about online privacy – actions inconsistent with attitudes. PRNewswire.


## BIGGEST LIE ON THE INTERNET

Turow, J, Hennessy, M and Draper, N (2015) The Trade Off Fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation.

University of Pennsylvania report.

Walker, JL (1966) A critique of the elitist theory of democracy. *American Political Science Review*, 60(2): 285-295.






Zogby International (2010) Results from interactive survey of adults, including a subset of parents with children age 18 and under. Comment to A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era Of Rapid Change, File No. P095416, comment number 00457.



[login](#) / [sign up](#)

# Drop that Name, get that job.

[LEARN MORE >>](#)





The future of professional networking services!

## Sign up now for FREE!

[JOIN!](#)

By clicking Join, you agree to abide by our terms of service.



[Contact](#) • [Careers](#) • [Terms of Service](#) • [Privacy Policy](#) • [About Us](#)

© Copyright NameDrop LLC. All rights Reserved.

Figure 1. Front page of fictitious SNS 'NameDrop'

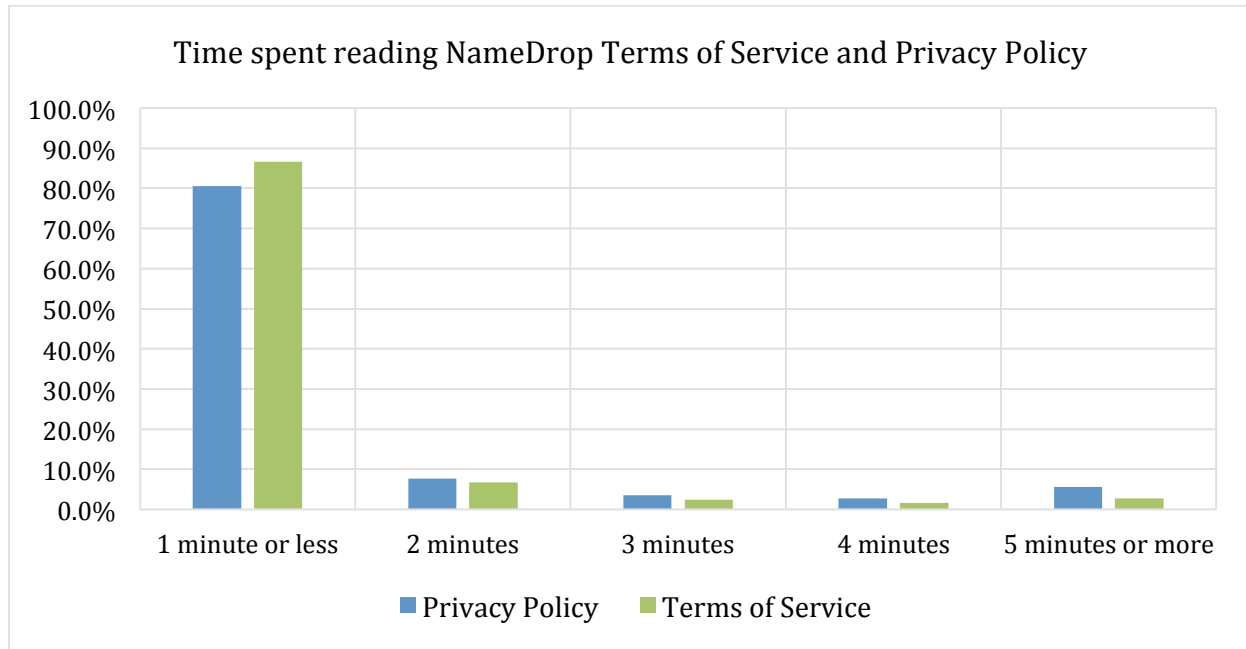


Figure 2. Time spent reading NameDrop Privacy Policy and Terms of Service.

Table 1. Policy attitudes factor analysis

Items	Factors and item loadings		
	Information overload	Nothing to hide	Difficult to understand
Privacy policies are too long	<b>.819</b>	.093	.088
There are too many privacy policies to read	<b>.802</b>	.149	.086
There are too many Terms of Service agreements to read	<b>.732</b>	.093	.086
Terms of Service agreements are too long	<b>.720</b>	.048	.073
I don't have time to read privacy policies for every site that I visit	<b>.630</b>	.203	.178
I don't have time to read Terms of Service agreements for every site that I visit	<b>.609</b>	.161	.177
It is normal to sign up for websites/apps without reading the Terms of Service agreements	<b>.593</b>	.145	.110
It is normal to sign up for websites/apps without reading the privacy policies	<b>.556</b>	.160	.153



## BIGGEST LIE ON THE INTERNET

Most people don't read Terms of Service agreements	<b>.539</b>	.086	-.050
Most people don't read privacy policies	<b>.526</b>	.119	-.022
Most people don't understand Terms of Service agreements	.455	.010	.428
I don't have time to read privacy policies	.445	.219	.195
I don't have time to read Terms of Service agreements	.420	.219	.241
I am not doing anything wrong, so what privacy policies say doesn't matter	.179	<b>.776</b>	-.029
I am not doing anything wrong, so what Terms of Service agreements say doesn't matter	.217	<b>.714</b>	-.044
The only users seriously affected by privacy policies are people who break the rules	.150	<b>.634</b>	-.149
Companies will never bother you whether you read their privacy policies or not	.115	<b>.626</b>	.042
Companies will never bother you whether you read their Terms of Service agreements or not	.127	<b>.581</b>	.000
The only users seriously affected by Terms of Service agreements are people who break the rules	.097	<b>.532</b>	-.215
I've got nothing to hide (privacy policies)	.269	<b>.517</b>	-.167
I've got nothing to hide (terms of service)	.250	<b>.501</b>	-.178
Companies will do what they want, regardless of whether I read the privacy policies	.096	.499	.188
It's important to read Terms of Service agreements to avoid trouble	-.007	-.483	-.252
It's important to read privacy policies to avoid trouble	.090	-.483	-.275
Companies will do what they want, regardless of whether I read the Terms of Service agreements	.096	.426	.129
The language in privacy policies is clear	-.133	.120	<b>-.711</b>
The language in Terms of Service agreements is clear	-.152	.133	<b>-.693</b>
Privacy policies are difficult to understand	.403	-.041	<b>.575</b>

# BIGGEST LIE ON THE INTERNET

Terms of Service agreements are difficult to understand	.437	-.069	<b>.537</b>
Most people don't understand privacy policies	.429	-.003	<b>.511</b>
Privacy policies provide helpful information	.100	-.355	-.450
Terms of Service agreements provide helpful information	-.030	-.278	-.440

Table 2. Final Regression Models Predicting Time Spent Reading Terms of Service and Privacy Policies upon Signup and when policies change

	Terms of Service						Privacy Policies					
	Upon sign up			When they change			Upon sign up			When they change		
	<i>B</i>	<i>SE B</i>	$\beta$	<i>B</i>	<i>SE B</i>	$\beta$	<i>B</i>	<i>SE B</i>	$\beta$	<i>B</i>	<i>SE B</i>	$\beta$
Age	.39	.16	.09*	-.07	.14	-.02	-.09	.18	-.02	-.22	.16	-.06
Gender	.19	.47	.02	-.05	.42	-.01	-.06	.52	-.01	-.46	.46	-.04
TOS reading	2.14	.31	.40***	1.57	.28	.37***	1.60	.34	.29***	1.36	.31	.28***
PP reading	.21	.29	.04	.09	.26	.02	1.19	.32	.24***	.62	.28	.14*
Information overload	-1.35	.41	-.17***	-1.54	.36	-.24***	-.40	.46	-.05	-1.54	.40	-.22***
Nothing to hide	.15	.22	.03	.23	.19	.06	-.01	.24	-.00	.17	.22	.04
Difficult to understand	.23	.22	.05	.29	.19	.07	-.05	.24	-.01	.24	.21	.05
Model $R^2$	.30***			.27***			.27***			.27***		

Note.  $p < .001$ . \* $p < .05$ , \*\* $p < .01$ , \*\*\* $p < .001$